REMARKS

No claims have been amended or canceled. Claims 1-13, 15-20, and 22-24 remain pending in the case. Further examination and reconsideration of pending claims 1-13, 15-20, and 22-24 are respectfully requested.

Section 103 Rejections

Claims 1-3, 8-13, 15-20, and 22-24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,047,067 to Rosen (hereinafter "Rosen") in view of U.S. Patent No. 5,768,385 to Simon (hereinafter "Simon"). In addition, claims 4-7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Rosen in view of Applied Cryptography by Schneier (hereinafter "Schneier"), and further in view of U.S. Patent Application 09/751,856 to Harif (hereinafter "Harif"). Applicant respectfully traverses this rejection in its entirety and incorporate by reference the arguments made in the previous Response to Office Action Mailed April 11, 2003 (hereinafter "Previous Response") with respect to Rosen. However, the newly cited reference to Simon will be addressed below along the allegations of a hypothetical combination of Rosen and Simon.

In order to sustain the Examiner's burden of showing a *prima facie* obviousness of a claimed invention, three essential criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. Second, there must be a reasonable expectation of success. As stated in MPEP 2143.01, the fact that references can be hypothetically combined or modified is not sufficient to establish a *prima facie* case of obviousness. *See In re Mills*, 916 F.2d. 680 (Fed Cir. 1990). Finally, the prior art references must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d. 981 (CCPA 1974); MPEP 2143.03, emphasis added. Specifically, "all words in a claim must be considered when judging the patentability of that claim against the prior art." *In re Wilson* 424 F.2d. 1382 (CCPA 1970). Using these standards, Applicant asserts that the cited art fails to teach or suggest all features of the currently pending claims. In addition, the cited art cannot be combined according to the hypothetical creation set forth in the Office Action since to do so would destroy the intended purpose of the references which explicitly teach away from that which is presently claimed. Some distinctive features of the present claims are set forth below.

Rosen and Simon do not teach, suggest, or provide motivation for maintaining the identities of the network members (i.e., network client, network host, or both) confidential to only the financial resolution unit. Present independent claims 1, 15, 19, 20, and 23 each recite the network client and network host have an identity that is confidential from one another -- i.e., the network client does not know the identity of the network host and vice-versa. As set forth in claim 19 and 23, a computational device can be either the network host (claim 19) or the network client (claim 23). Moreover, claim 1 makes clear that even though the other independent claims specify the network client does not know the identity of the network host and vice-versa, the the identity of the network client and network host are known only to the financial resolution center. The financial resolution center is described throughout the specification not as a network client 12 or a network host 16, but as, for example, a financial institution (Specification -- Fig. 1; pg. 14, line 14-21).

From reviewing the cited art, it appears that a brief description of the present specification is needed to help demarcate that which is claimed from Rosen, Simon, or a combination thereof. As set forth in the present specification, computing resources are very expensive to "acquire and maintain" (Specification -- pg. 6, lines 24-28). Thus, it would be desirable to make available intensive data processing and computing resource allocation to users who, "on their own, would never be able to buy, maintain, or staff the data centers necessary to perform intensive data processing" (Specification -- pg. 7, lines 8-11).

To achieve this benefit, a network server will "act as an intermediary between a client and a host in negotiating a price for the execution of a process" (Specification -- pg. 8, lines 9-14). The network server will receive a payload that contains a specification of a particular process requiring execution by a computing system -- that process being attributable to or associated with a task (Specification -- pg. 13, lines 4-24). Once the payload and specification for the process is received by the network server from the network client, the network server can then solicit bids from a network host, for that host to then execute the process (Specification -- pg. 17, lines 26-28). The bids solicited by the network server are indicative of a dollar amount that a network host would charge, in terms of computing resources needed, to execute that particular process being solicited. For example, a corporation such as IBM Corporation might actually sell computing resources to smaller users of those resources; thus, the smaller users would be required to pay IBM in terms of, for example, computing time.

The process by which money exchanges hands takes place primarily through a financial clearinghouse, such as a financial resolution center (FRC) (Specification – Fig. 1). In order for the network client to pay the network host provider for executing the client's program, the network client 12 will issue, along with payload 30, a network client program instruction 42 and, more particularly, a financial charge receiving program 424 (Specification – Figs. 1-2). Upon sending payload 30, however, network client 12 only knows the identity of the network server, and the network server 14 will negotiate independent of client 12 with various network hosts to solicit bits from those network hosts 16 (Specification – pg. 17, line 23 - pg. 18, line 2; Fig. 1). Once network server 14 accepts a bid from a particular host 16, payload 30 is forwarded from server 14 to host 16 in order for host 16 to execute the program (Specification – pg. 18, lines 4-11). Throughout the process, however, the network client does not know the identity of the network host or vice-versa. All client 12 does is forward a payload specifying execution of a program, and it is then up to the network server 14 to solicit bits. Thus, the network client communicates with the network server, but no further; the network server communicates with a network host. Importantly, the network server, as an intermediary, prevents disclosing identities of the network client to a network host or vice-versa. The network server simply forwards a specification from a client and receives bid proposals and executed outcomes from a host.

Along with network server 14, a financial resolution center also operates as an intermediary on financial transactions, where money is paid from the client to the host. The client, however, does not know the identity of a host that has performed services for that client. Instead, the network server has a transmission medium 26 extending between itself and FRC 22 (Specification – Fig. 1). Network server 14 thereby instructs the financial resolution center to submit, for example, a request for payment from the network server to the network client and, thereafter, FRC 22 forwards electronic funds received from the client either directly to host 16 or to host 16 via network server 14 (Specification – pg. 18, line 13 - pg. 21, line 20). To impart integrity into the overall system, it is important that the client not know the identity of the host which performs processing services for the client, and the host not know which client requested those services. It is also important that the FRC provide anonymous payments from the network server to the network host without the host knowing that the payment was derived from a network client (See, for example, Specification – pg. 8, lines 17-25). Further details of both the processing request, bid procedure, and processing transaction, as well as the financial exchange resulting from the processing transaction was provided in the Previous Response – particularly, pages 9-10.

Contrary to the claimed anonymity between a network client and the network host, Rosen specifically requires the identity of subscriber A be disclosed to subscriber B and vice-versa. For example, Rosen states that "A agrees to exchange with B dollars ($) for pounds (£) at an exchange rate of $/£" (Rosen – col. 16, lines 53-54). Therefore, a client (i.e., subscriber A) in Rosen must be aware of the identity of a host (i.e., subscriber B) if it agrees to exchange currency specifically with B. Rosen also states that in a point of sale (POS) payment protocol, "A agrees to purchase products or services from B" (Rosen – col. 19, line 45). Thus, Rosen specifically requires that for a transaction between a client and a host, A must know the identity of B since A agrees to purchase goods or services specifically from B! Therefore, Rosen purposely teaches away from the anonymity or confidentiality requirements of the present independent claims (See, Previous Response – pp. 10-12).

Therefore, Applicant cannot agree with the statement made on page 2 of the Office Action that "Rosen ('067) does not explicitly disclose identities of the network members are known only to the financial resolution center." A person skilled in the art, when reading Rosen, would not deduce that Rosen simply "does not explicitly disclose identities of the network members are known only to the financial resolution center," but would gather from Rosen's teachings that Rosen specifically requires that the network members must be known to each other in order for the transaction to occur. There simply is no intermediary in Rosen that could solicit bids from a client and submit payment from the client, completely anonymous to the host and vice-versa. Currency exchange transactions and point of sale transactions simply do not work in the fashion presently claimed.

The deficiencies of Rosen are further compounded by the deficiencies of the newly cited reference to Simon. A closer reading of Simon will make clear that the customer 10 (spender/payor) must communicate with vendor 20 (payee) (Simon – col. 7, lines 29-32; col. 4, lines 55-56). In order to exchange money from a customer 10 to a vendor 20 via bank 30, a pre-image x_1 must be sent from the customer 10 to vendor 20 (Simon – col. 7, 30-32, emphasis added). The pre-image x_1 is simply a random number generated by a customer associated with a particular transaction for which that customer must pay (Simon – col. 5, lines 59-61). Customer 10 will keep the pre-image x_1 secret until payment takes place (Simon – col. 5, lines 64-65). Customer 10 then supplies the customer's bank 30 the pre-image x_1, and another image of a function $f(x_2)$ (Simon – col. 6, lines 58-60). The function of the pre-image is an "unblinded" form of the image, where all third parties can view that function (Simon – col. 3, lines 6-8). As the pre-image is forwarded to the bank, customer 10 also forwards the pre-image to the vendor receiving party (Simon – col. 7, lines 30-32, emphasis added).

Armed with the pre-image, vendor 20 will then send the pre-image along with the function $f(x_1)$ to the customer's bank 30, requesting the bank to release or credit vendor 20 with payment (Simon -- compare Figs. 1 and 4). The pre-image x_1 thereby suffices as a randomly generated key, and the only subscribers who know that key are customer 10, bank 30, and vendor 20. Importantly, according to the teachings of Simon, the identity of a vendor must be known to the customer since it would be impossible for the customer to forward the pre-image x_1 to the vendor without knowing the vendor's identity! If the customer did not know the identity of the vendor in Simon, then the pre-image key could not be exchanged and no funds could be transferred. Thus, if a client is anonymous to a host and vice versa as claimed, then exchange of payment in Simon would be impossible. Simon begins and ends with the exchange of the private key, known as the pre-image; absent the exchange between a client and host, funds could not be transferred as taught by Simon. Thus, Simon suffers the same deficiencies as Rosen in that the client and host must know each other in order to complete the arm's length transaction. The particular purchase and sale of computer resources as claimed, however, does not require this form of arm's length transaction; thus, the identities of the presently claimed client and host need not by disclosed to each other and can simply reside in the FRC or network server.

For at least the reasons set forth above, independent claims 1, 15, 19, 20, and 23, as well as claims dependent therefrom, are asserted to be patentable over Rosen and Simon, either individually or in combination. Accordingly, removal of this rejection is respectfully requested.
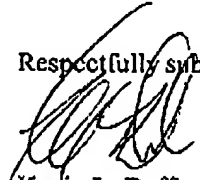
In addition, several of the dependent claims are believed to be separately patentable. For example, claim 2 recites in part: ". . . wherein the network members are determined by the financial resolution center." This feature in combination with the features of independent claim 1 do not appear to be taught or suggested by the prior art. Furthermore, the cited references (Schneier and Harif) to various dependent claims, such as claims 4-7, do not individually or in combination render those claims, as further limitations of claim 1, obvious.

CONCLUSION

This response constitutes a complete response to all issues raised in the Office Action mailed April 7, 2004. In view of the remarks traversing the rejections presented therein, Applicants assert that pending claims 1-13, 15-20, and 22-24 are in condition for allowance. If the Examiner has any questions, comments, or suggestions, the undersigned attorney earnestly requests a telephone conference.

SN 09/751,856 Response to Office Action Mailed 4/7/2004   Page 6 of 7

PAGE 6/7 * RCVD AT 7/6/2004 4:53:08 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:5127031250 * DURATION (mm-ss):04-22

No fees are required for filing this amendment; however, the Commissioner is authorized to charge any additional fees which may be required, or credit any overpayment, to Conley Rose, P.C. Deposit Account No. 03-2769/5468-06500.

Respectfully submitted,

Kevin L. Daffer
Reg. No. 34,146
Attorney for Applicant(s)

Conley Rose, P.C.
P.O. Box 684908
Austin, TX 78768-4908
Ph: (512) 476-1400
Date: July 6, 2004

SN 09/751,856 Response to Office Action Mailed 4/7/2004   Page 7 of 7

PAGE 7/7 * RCVD AT 7/6/2004 4:53:08 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:5127031250 * DURATION (mm-ss):04-22